CyberBlueSOC

Your Blue Team Security Lab

Installation & User Guide

CyberBlueSOC · October 2025 · CyberBlue.co · Version 1.0

Table of Contents

Table of Figures

Welcome to CyberBlueSOC

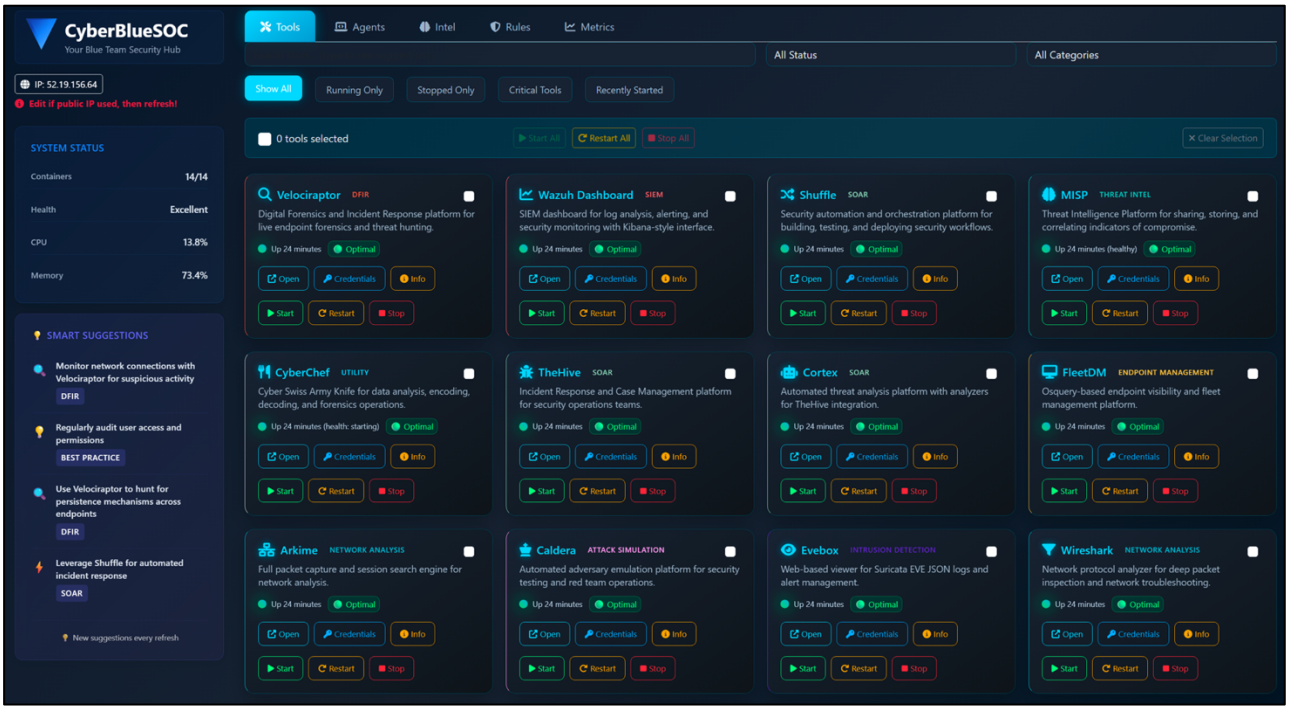
Your Complete Security Operations Center

What is CyberBlueSOC?

CyberBlueSOC transforms your Ubuntu machine into a SOC Blue Team LAB in less than an hour - with the same enterprise tools used by Security Operations Centers and Blue Team Labs.
No complexity . No licenses

What You Get:

- Enterprise SIEM platform (Wazuh)
- DFIR – EDR Endpoint investigation (Velociraptor)
- Incident response platform (TheHive & Cortex)
- Security automation (Shuffle)
- Attacks Simulation (Caldera)
- 250,000+ threat indicators (MISP)
- Network forensics tools (Arkime, Wireshark)
- + additional professional tools
- Beautiful web portal - no password required



The Problem It Solves

Traditional security tool deployment:

- Takes weeks to configure
- Requires licenses
- Tools don't integrate
- Endless troubleshooting

CyberBlueSOC makes it:

- About 30-minute setup
- Using open-source
- integrated & Works out-of-the-box.

Who This Is For

- Security Students → Build job-ready skills SOC Analysts → Practice with real tools
- Career Changers → Get hands-on experience IT Professionals → Add security expertise

Your 15+ Security Tools

SIEM & Monitoring:

- **Wazuh** - Enterprise SIEM dashboard
- **Suricata** - Network intrusion detection
- **EveBox** - Real-time security events

Digital Forensics:

- **Velociraptor** - Endpoint investigation
- **Arkime** - Network traffic analysis
- **Wireshark** - Protocol analyzer

Threat Intelligence:

- **MISP** - 250,000+ threat indicators
- **MITRE ATT&CK** - Threat modeling

Incident Response:

- **TheHive** - Case management
- **Cortex** - Artifact analysis
- **Shuffle** - Security automation

Attacks Simulations

- **Caldera** - Adversary emulation

Utilities:

- **CyberChef** - Data analysis
- **Fleet** - Endpoint management
- **Portainer** - Container management

Threat Hunting:

- **YARA** - 523+ malware detection rules
- **Sigma** - 3,047+ SIEM detection rules

Quick Installation

Simple Commands:

Installation Commands

```
git clone https://github.com/CyberBlu3s/CyberBlue.git
cd CyberBlue
chmod +x cyberblue_install.sh
./cyberblue_install.sh
```

That's it! The installer runs completely automatically for 30-45 minutes.

System Requirements

Recommended Specifications

CPU: 8+cores(Intel/AMDx86_64)

RAM: 16GB minimum

Disk: 150GB+ SSD **OS:** Ubuntu22.04+

Runs on: · VMware · VirtualBox · Cloud VMs (AWS) · etc

Installation Process

The fully automated installer handles everything:

Phase 1 (10-15 min): System setup

- Installing Docker & Docker Compose
- Configuring 8GB swap space
- Installing YARA (523+ rules) & Sigma (3,047+ rules)
- System optimizations

Phase 2 (15-20 min): Deployment

- Building 30+ containers
- Configuring networks and Generating SSL certificates
- Downloading agent binaries

Phase 3 (5-10 min): Configuration

- Enabling auto-start on reboot
- Final health checks

☕ *Grab a coffee and watch the automated installation!*

Your CyberBlueSOC Portal

Instant Access - No Password!

After installation, simply open your

browser: **https://YOUR_SERVER_IP:5443**

SSL Certificate Warning

You'll see a security warning about the certificate. This is normal for lab environments.Click **Advanced→Proceed** (safe in your isolated lab)

No login required! The portal opens directly - perfect for quick lab access.

Portal Interface Overview

Your portal has 5 main tabs visible at the top:

1. **Tools Tab** (Default view)
   - Manage all 15+ security tools
   - Start/Stop/Restart controls
   - View credentials for each tool

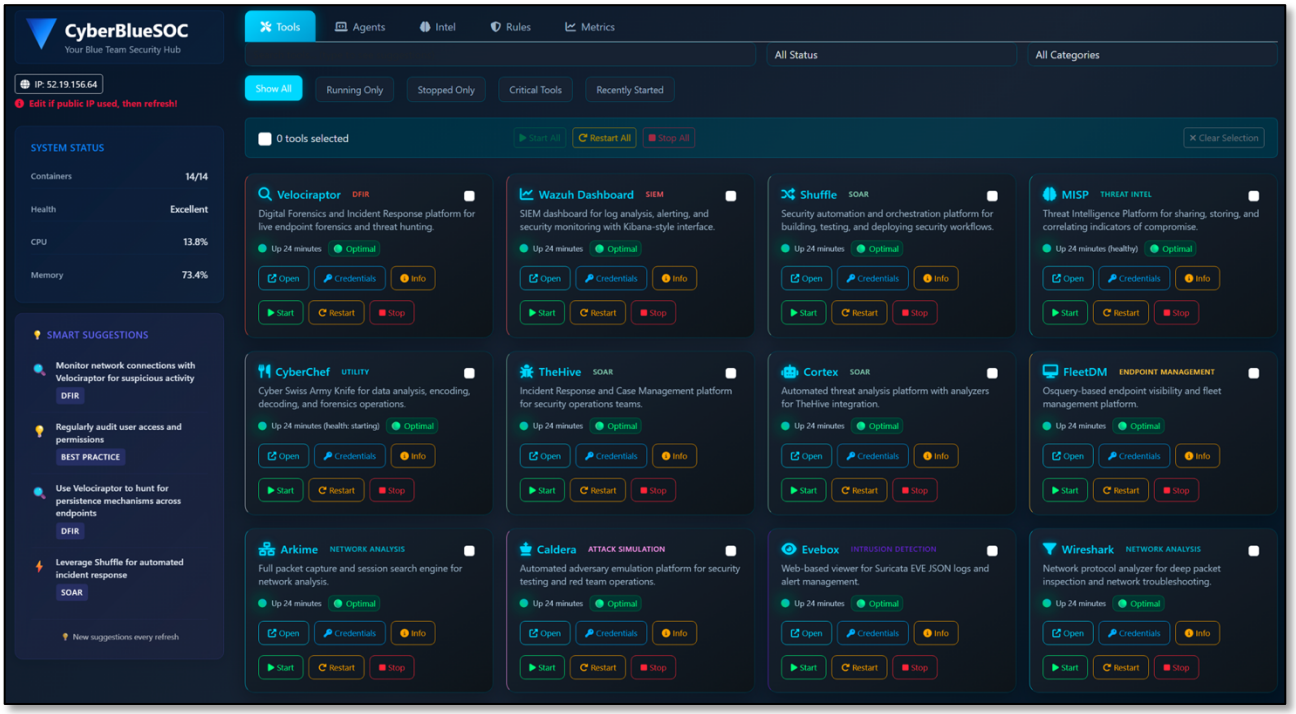


Figure 1: CyberBlueSOC Dashboard

2. Agents Tab

- Deploy Velociraptor to Windows/Linux/macOS
- Deploy Wazuh agents
- Start network captures with Arkime

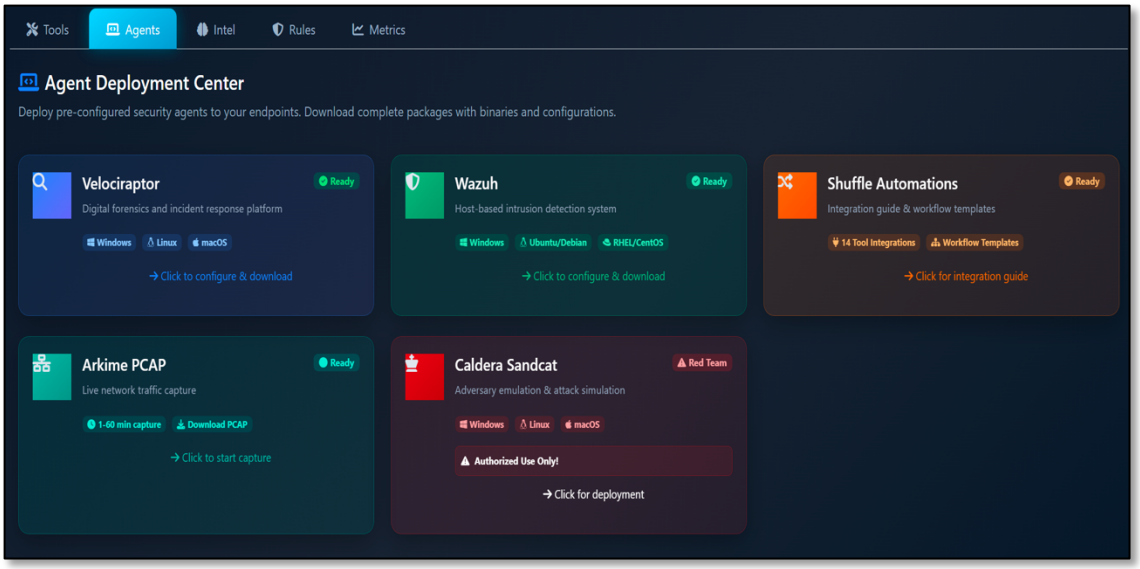


Figure 2: CyberBlueSOC Agents Deployment Dashboard

3. Intel Tab

- Search 200,000+ threat indicators
- Query IPs, domains, hashes
- View MISP statistics
- See recent threat events

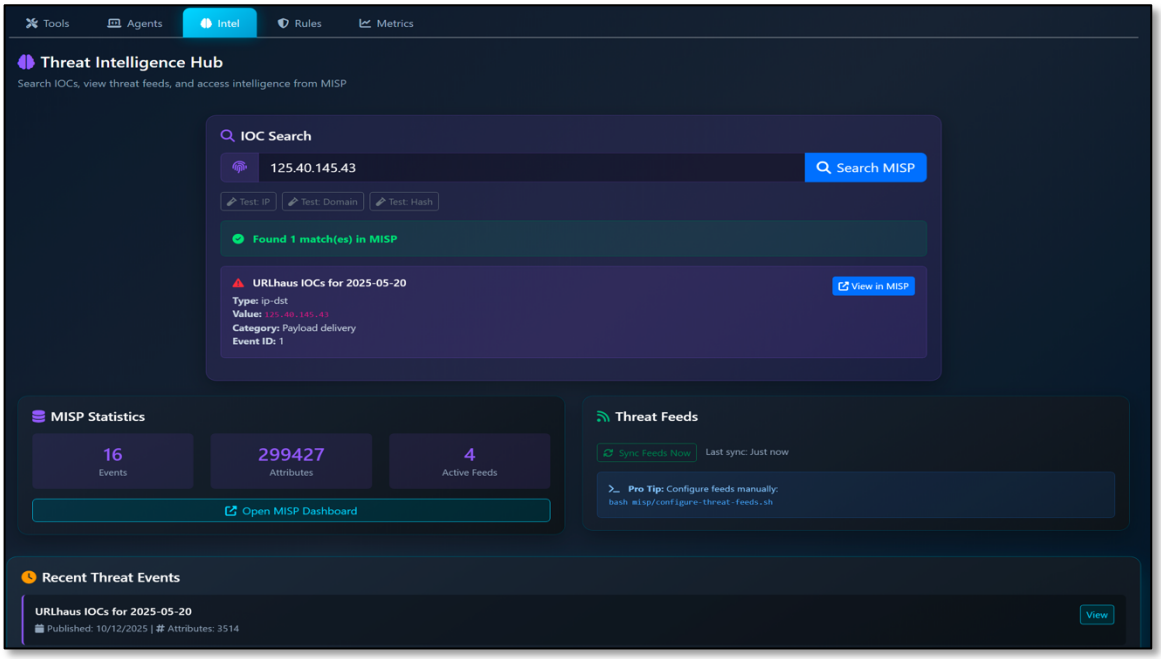


Figure 3: CyberBlueSOC Intel Dashboard

4. Rules Tab

- Browse 523 YARA malware rules
- Browse 3,047 Sigma detection rules
- View rule content
- Copy rules to clipboard

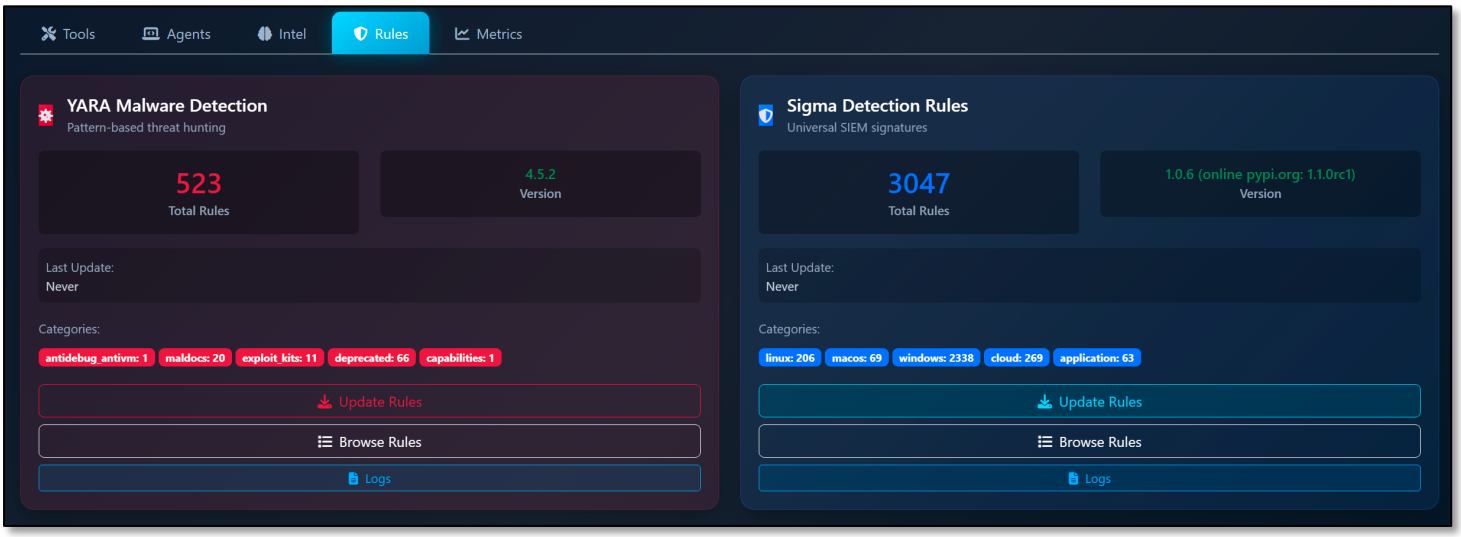


Figure 4: CyberBlueSOC Rules Dashboard

5. Metrics Tab

- System performance dashboard
- Container health monitoring
- Network statistics
- Recent events
  - Visual grid showing all 30+ containers

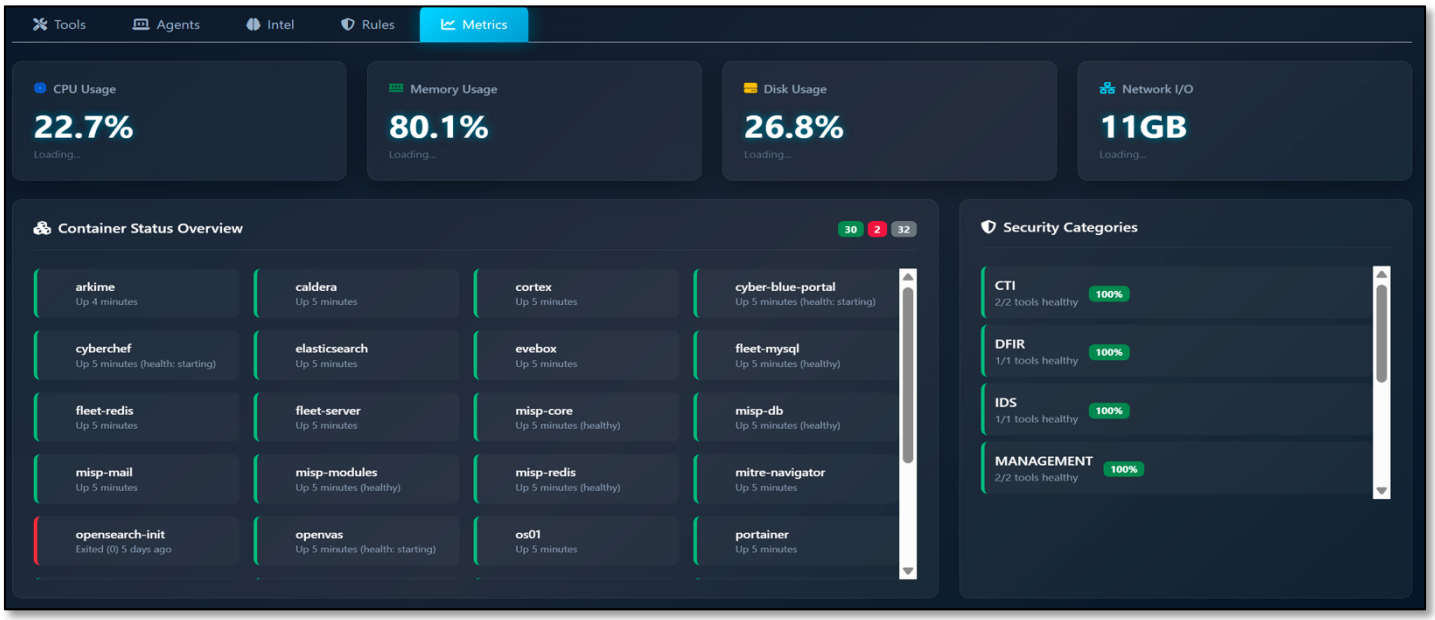


Figure 5: CyberBlueSOC Metrics Dashboard

Tool Cards Explained

Each security tool appears as a card with:

Header: Tool name + Category badge (SIEM/DFIR/CTI/SOAR)

Status: Green "Up X minutes" or Red "Stopped"

Description: What the tool does

Controls:

- Open - Launch tool in new tab
- Credentials - Show login info popup
- Info - Detailed information
- Start / Restart / Stop - Management buttons

The main dashboard displays multiple tool cards in a clean grid layout, each showing real-time status and instant access controls.

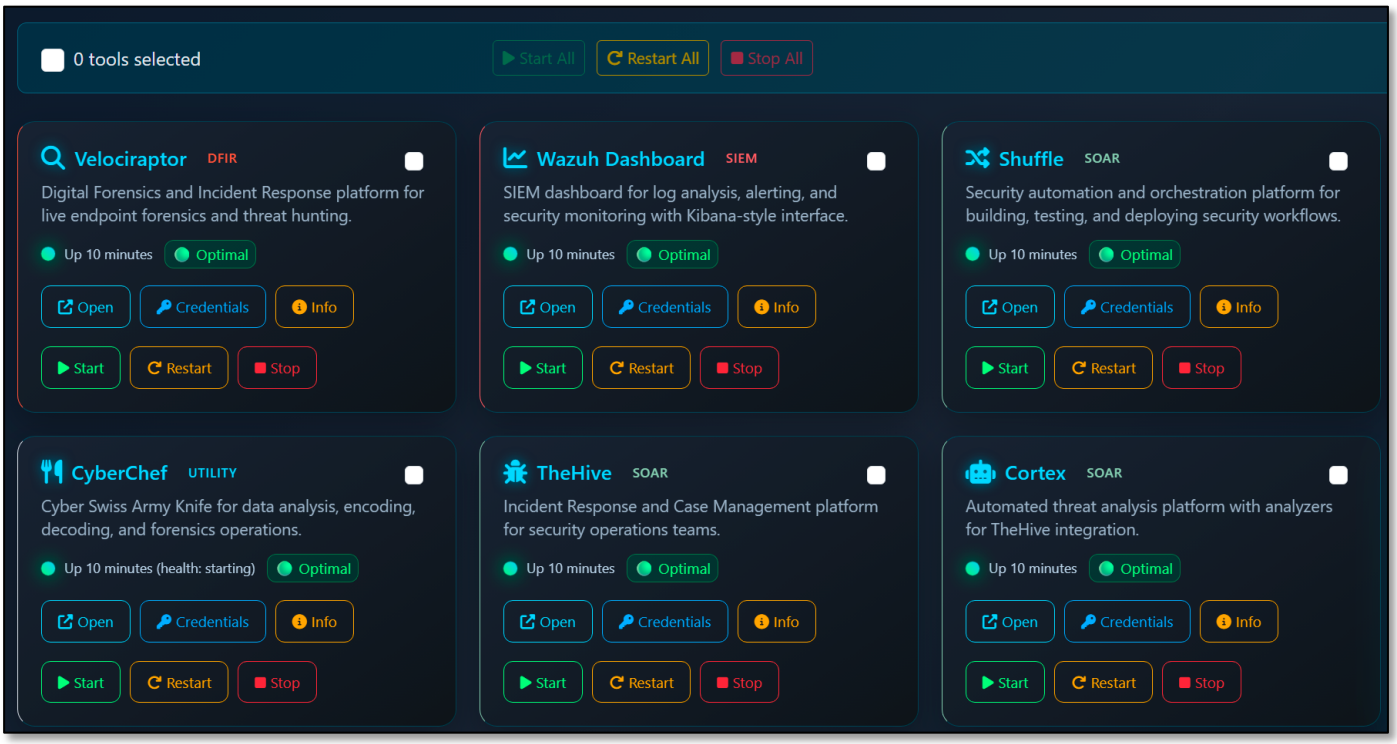


Figure 6: Tools Cards

Viewing Tool Credentials

Click the **Credentials** button on any tool card to see a popup with:

- Access URL (with copy button)
- Username and password
- Container status

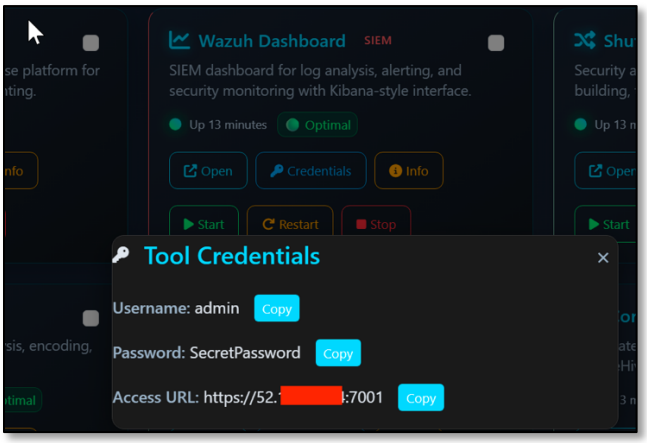


Figure 7: Tools Credentials

Viewing Tool Information

Click the **Information** button to see more details about the container status, Access, and quick start guide.

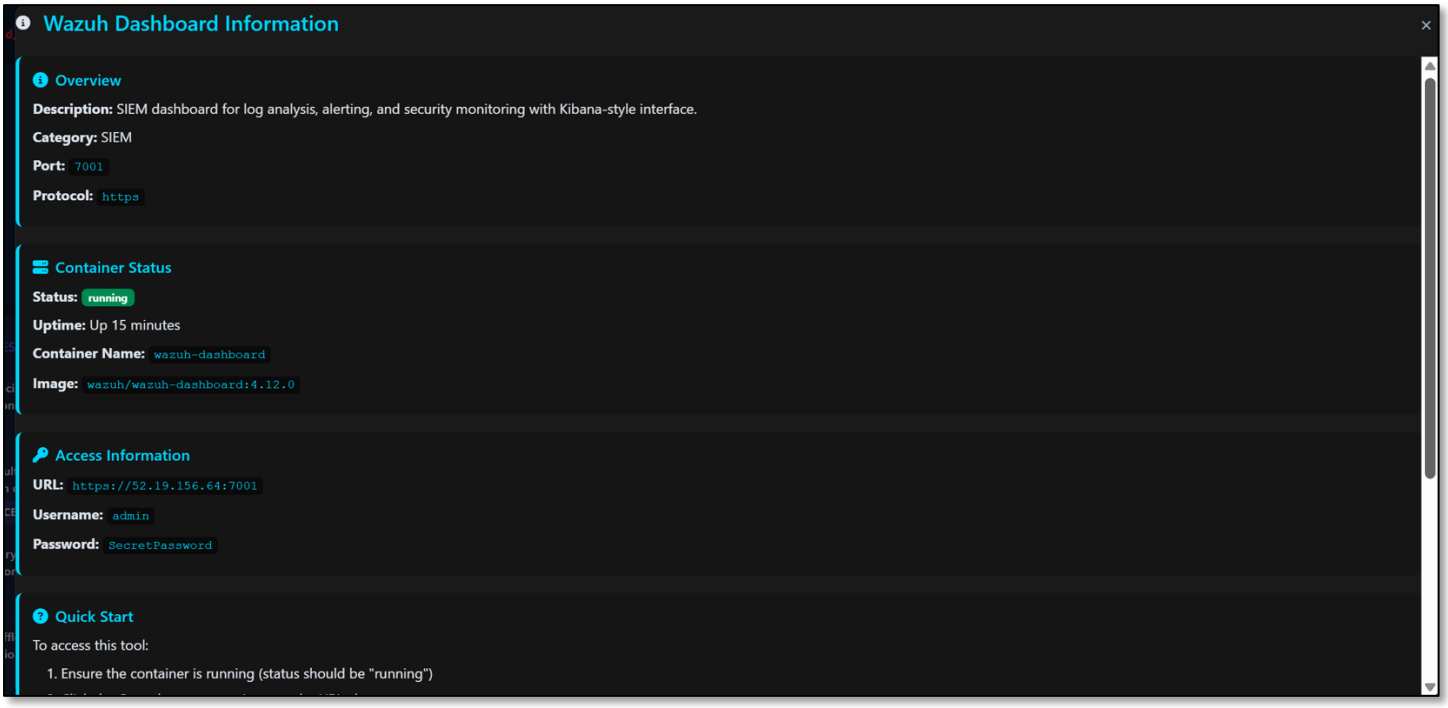


Figure 8: Tools Information feature

Tool Access Guide

All Your Tools (No Portal Password!)

QuickAccess

Portal has **no authentication**- just open and use!
https://YOUR_IP:5443 → Direct access to dashboard

Complete Tool List

Tool	URL	Credentials
CyberBlueSOC Portal	https://IP:5443	No password!
Velociraptor	https://IP:7000	admin / cyberblue
Wazuh	https://IP:7001	admin / SecretPassword
Shuffle	https://IP:7002	admin / password
MISP	https://IP:7003	admin@admin.test / admin
CyberChef	http://IP:7004	No auth
TheHive	http://IP:7005	admin@thehive.local / secret
Cortex	http://IP:7006	admin / cyberblue123
Fleet	http://IP:7007	Setup on first use
Arkime	http://IP:7008	admin / admin
Caldera	http://IP:7009	red / blue: cyberblue
Wireshark	https://IP:7099	admin / cyberblue
ATT&CK Navigator	http://IP:7013	No auth
EveBox	http://IP:7015	No auth
Portainer	https://IP:9443	admin / cyberblue123

Replace IP with your server's IP address from installation

Verify the Access to Tools

Velociraptor (EDR/DFIR)

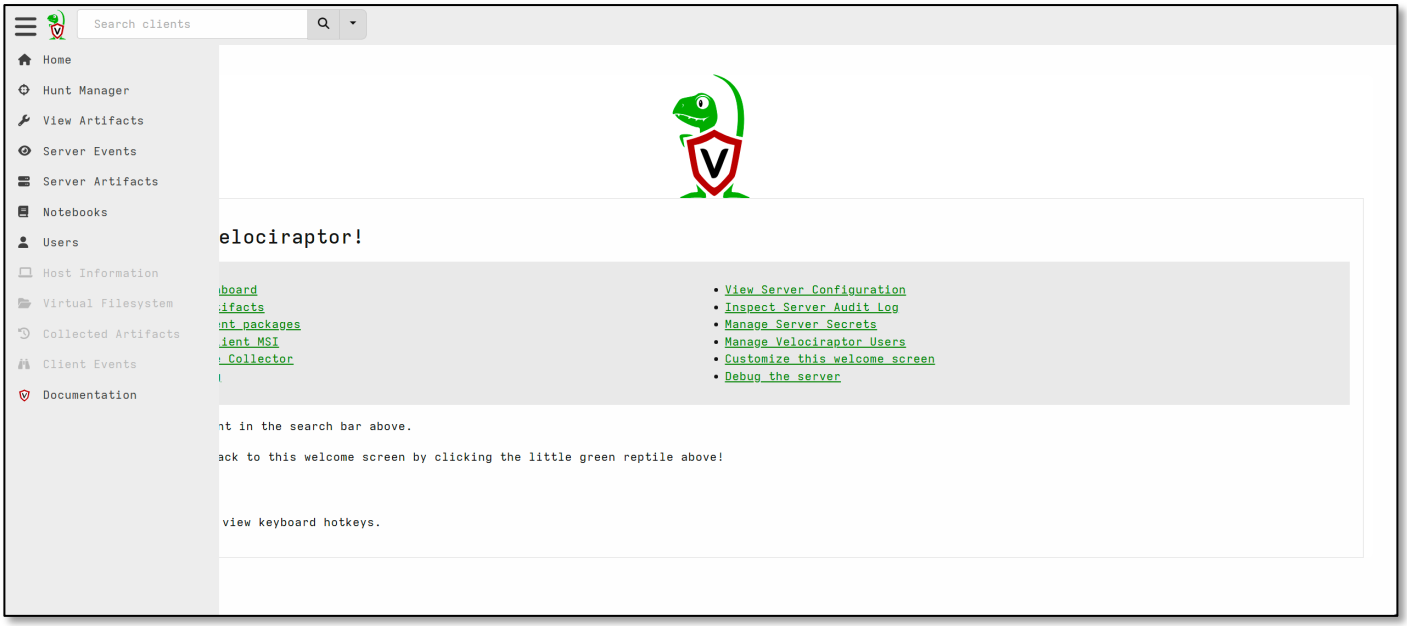


Figure 9: Velociraptor WebUI

Wazuh (SIEM)

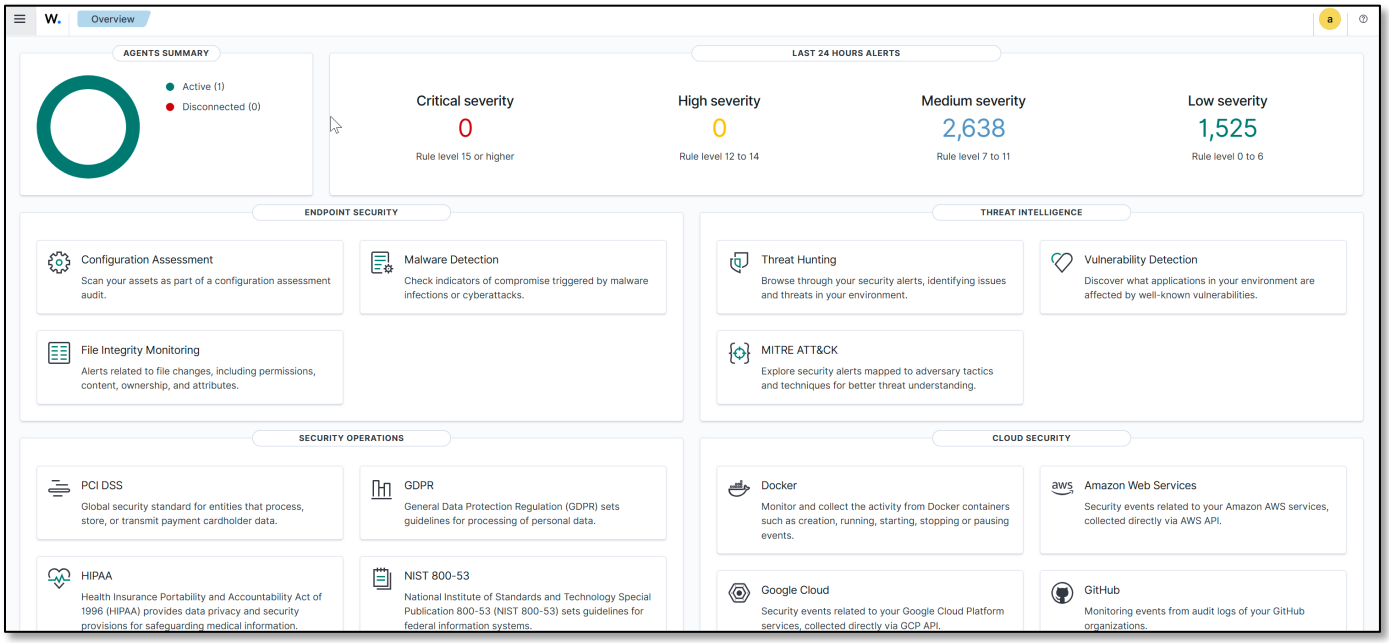


Figure 10: Wazuh WebUI

Shuffle (SOAR)

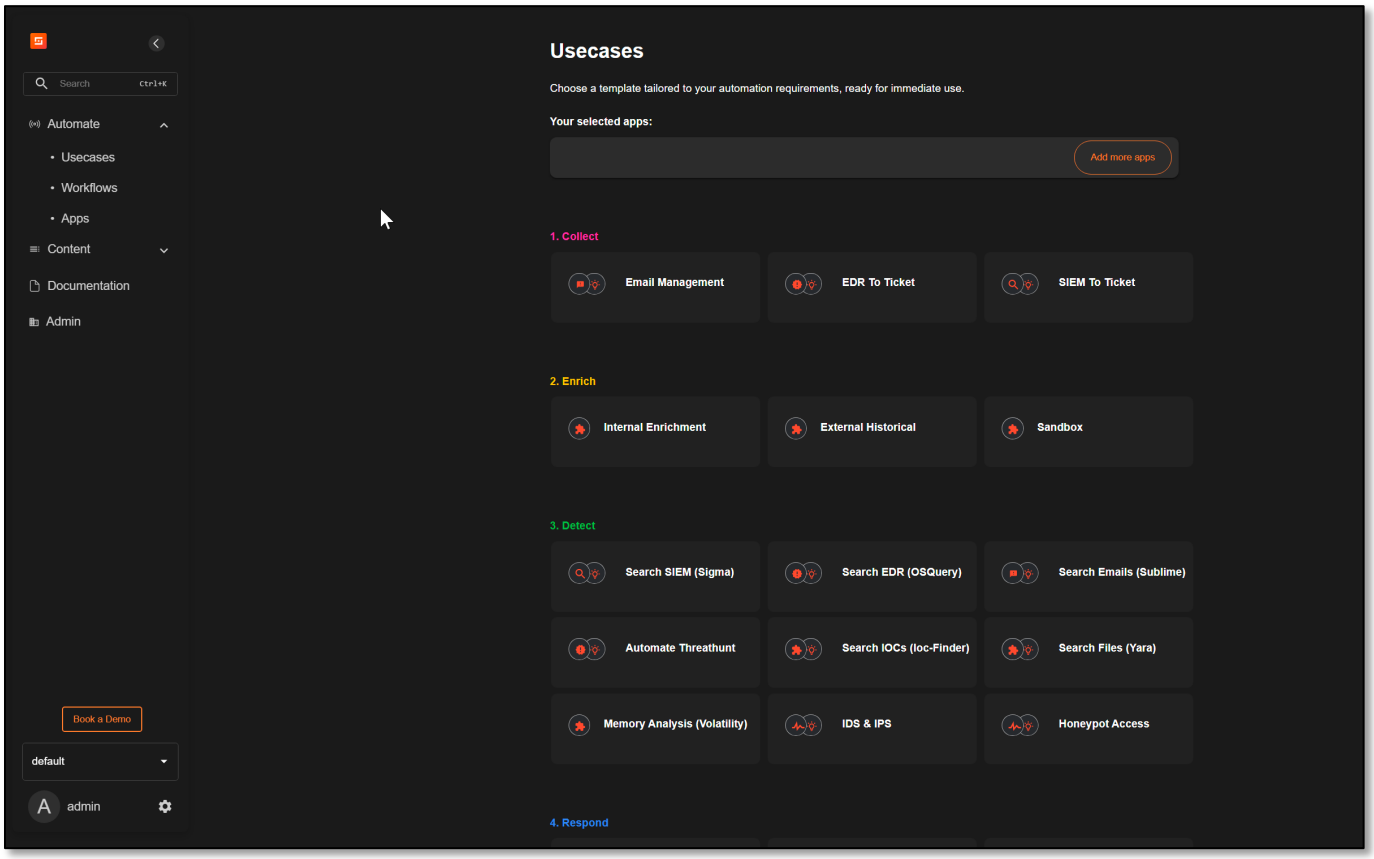


Figure 11: Shuffle WebUI

MISP (Threat Intel)

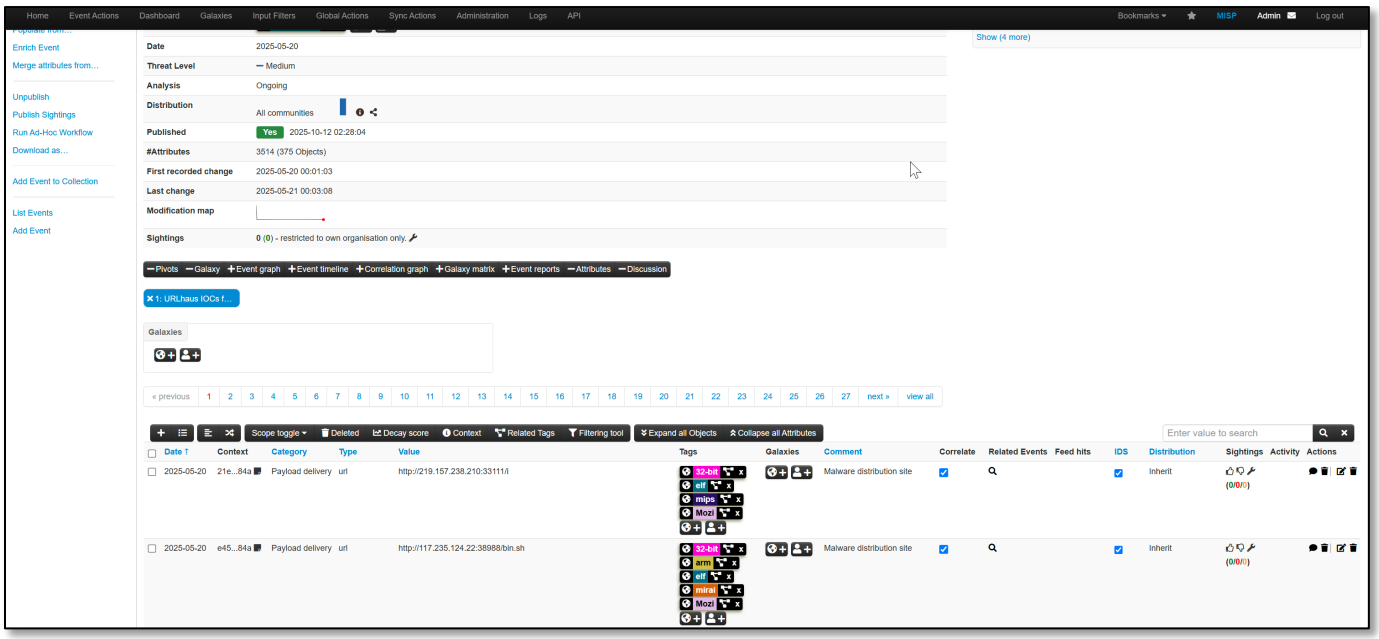


Figure 12: MISP WebUI

CyberChef (Utility: Swiss Army Knife)

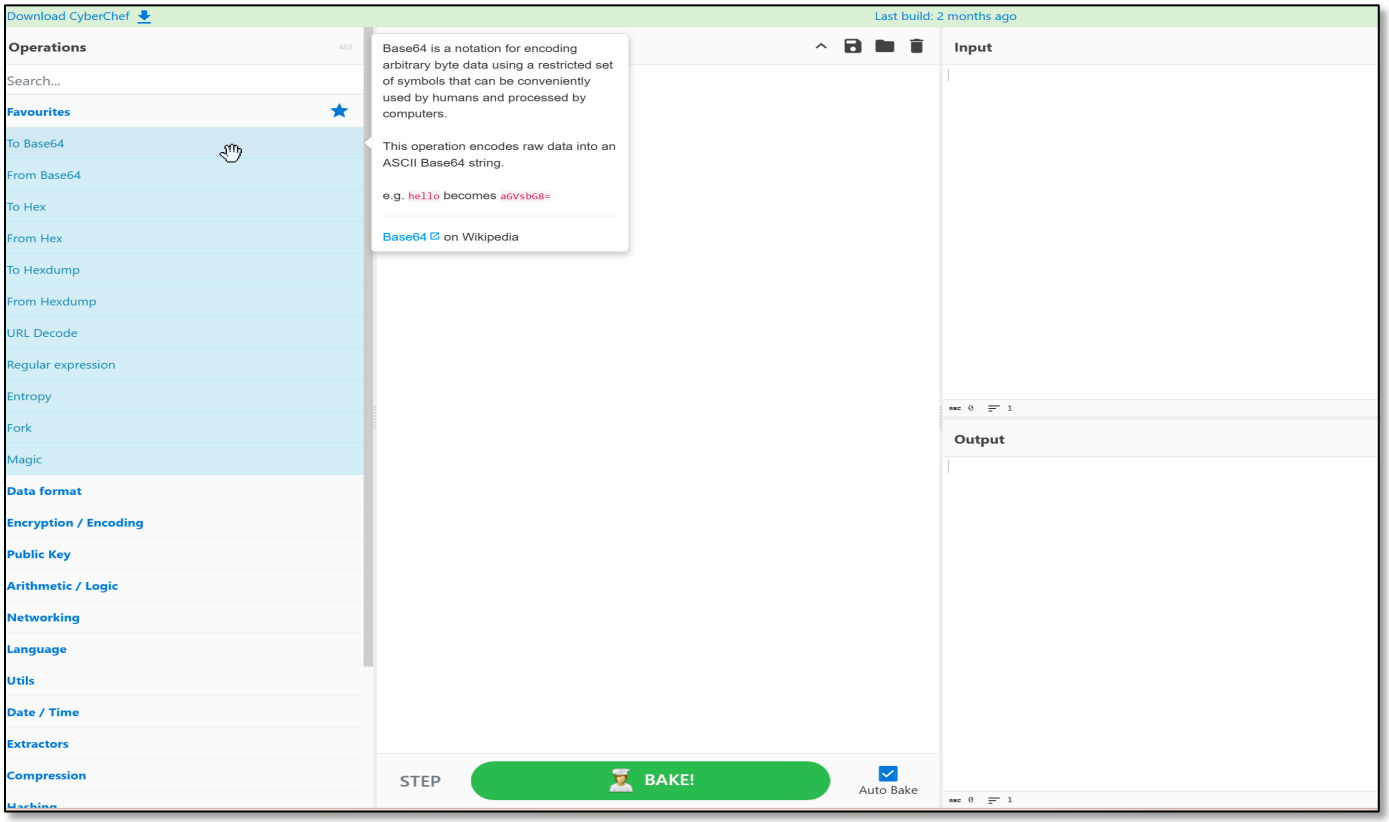


Figure 13: CyberChef WebUI

TheHive (Case Management)

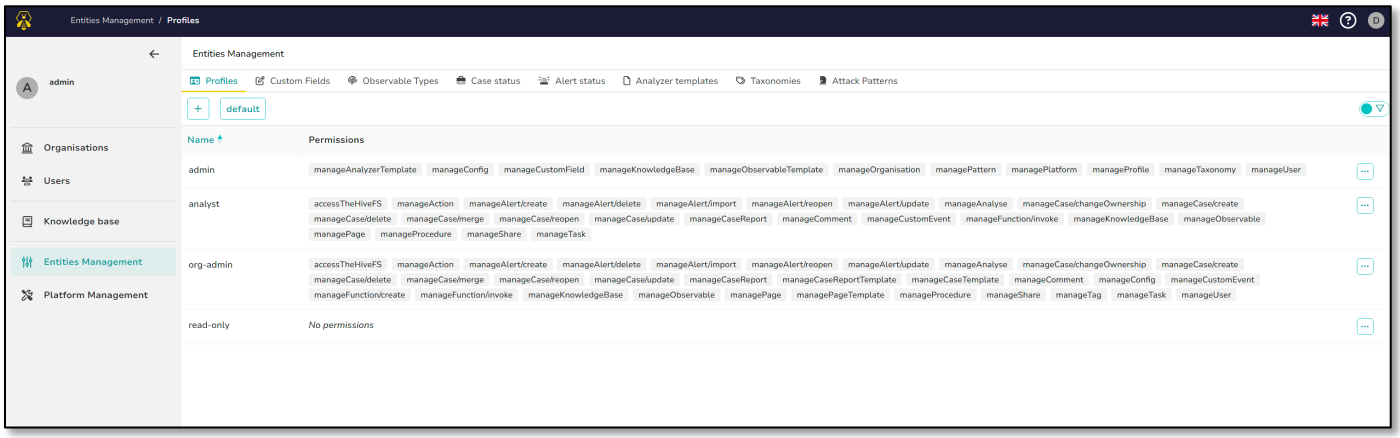


Figure 14: TheHive WebUI)

Cortex (The Hive observables Analyzer)

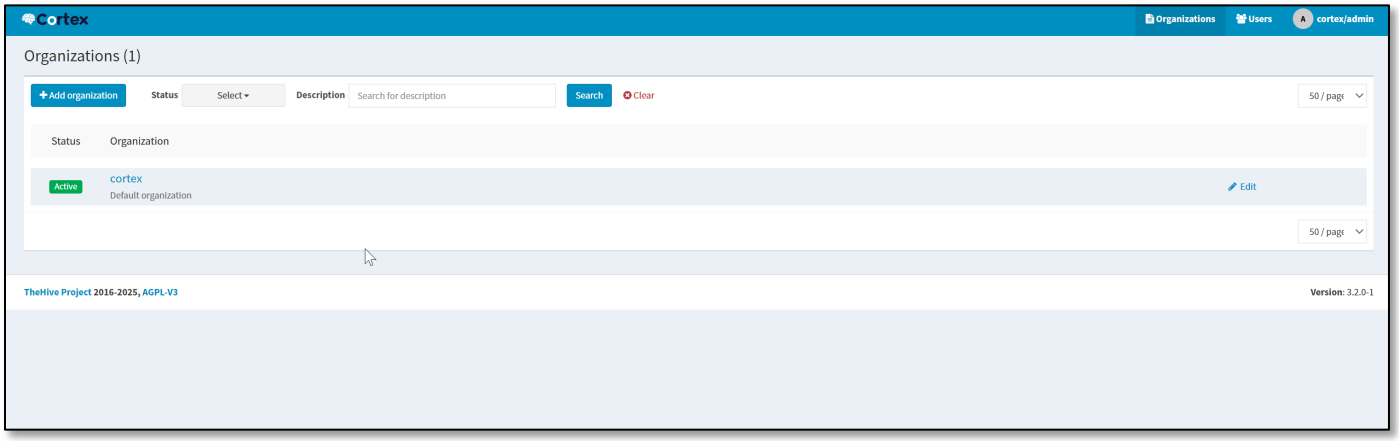


Figure 15: Cortex WebUI

Fleet (Device Management – Osquery)

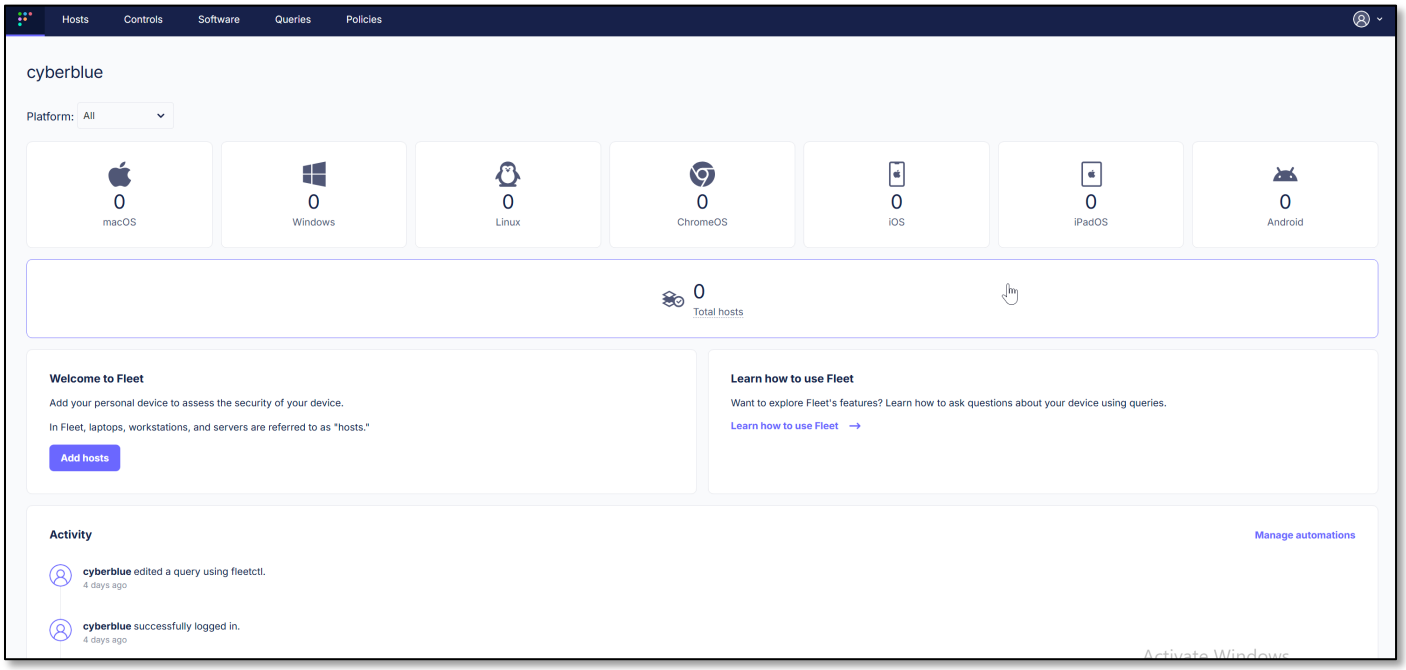


Figure 16: FleetDM WebUI

Arkime (packet capturing)

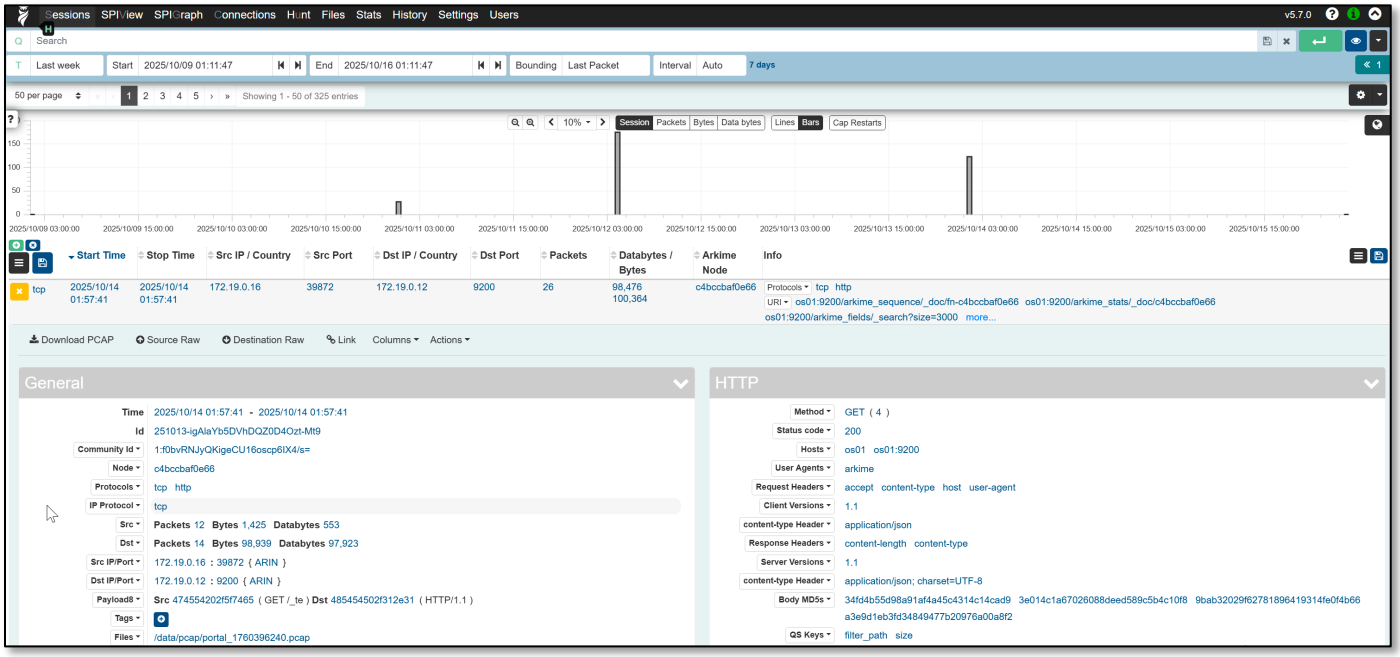


Figure 17: Arkime WebUI

MITRE Caldera (adversary emulation)

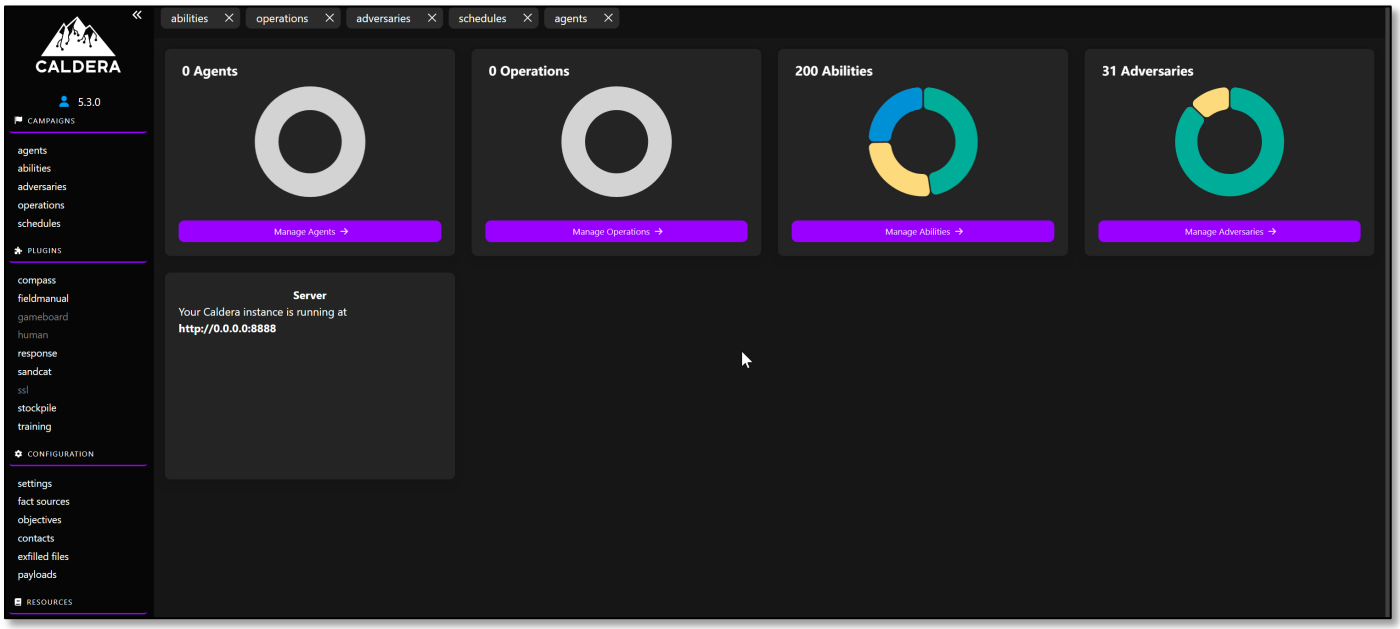


Figure 18: MITRE Caldera WebUI

EveBox (Suricata alert and event management)

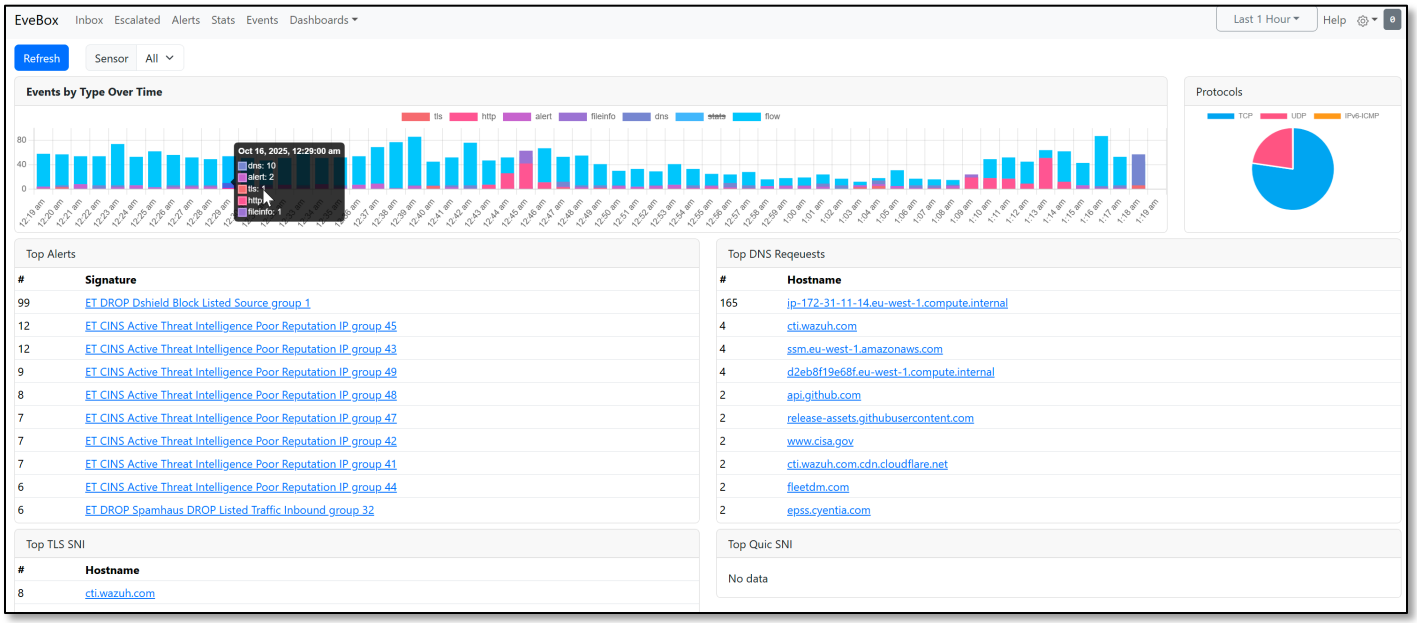


Figure 19: EveBox WebUI

Wireshark (Network Analysis)

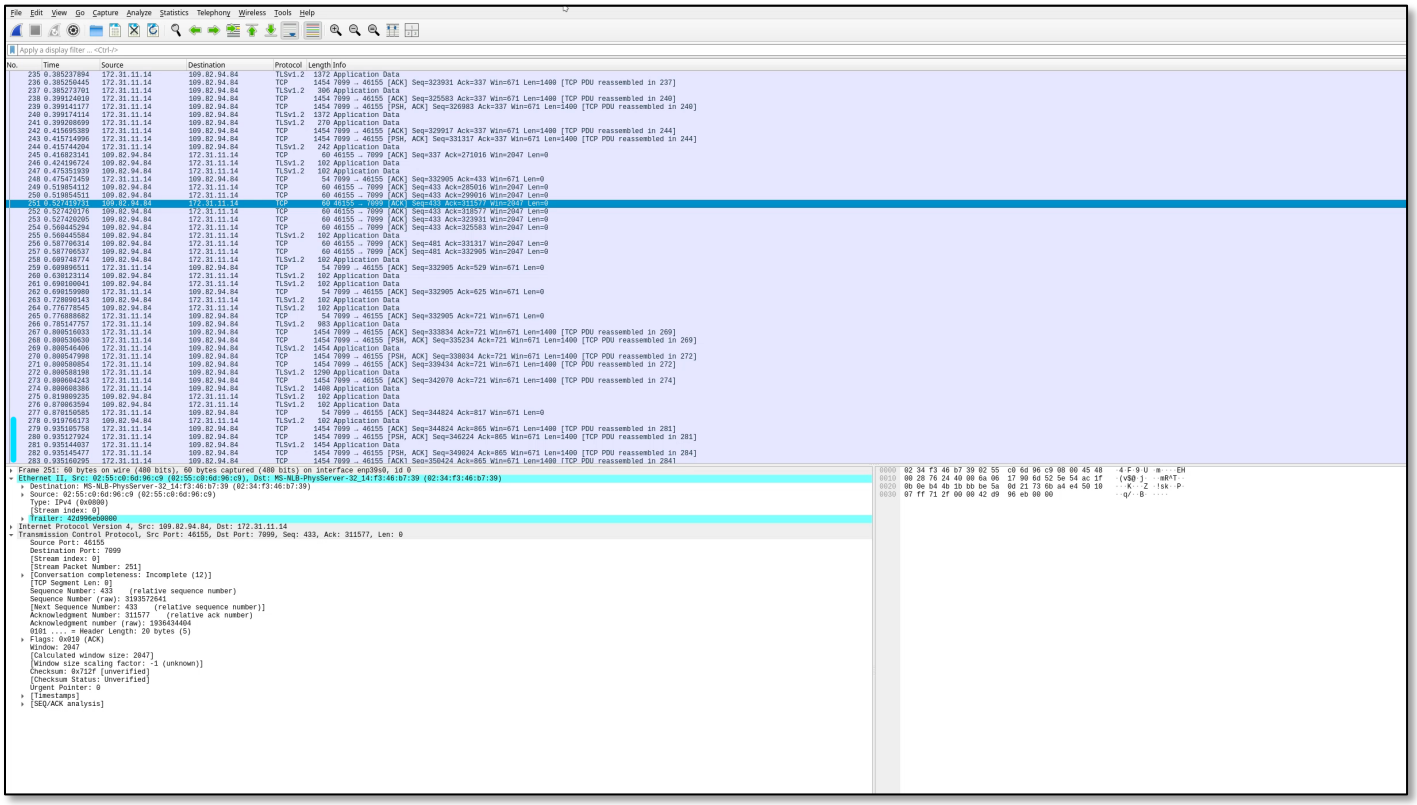


Figure 20: Wireshark WebUI

ATT&CK Navigator (ATT&CK matrices)

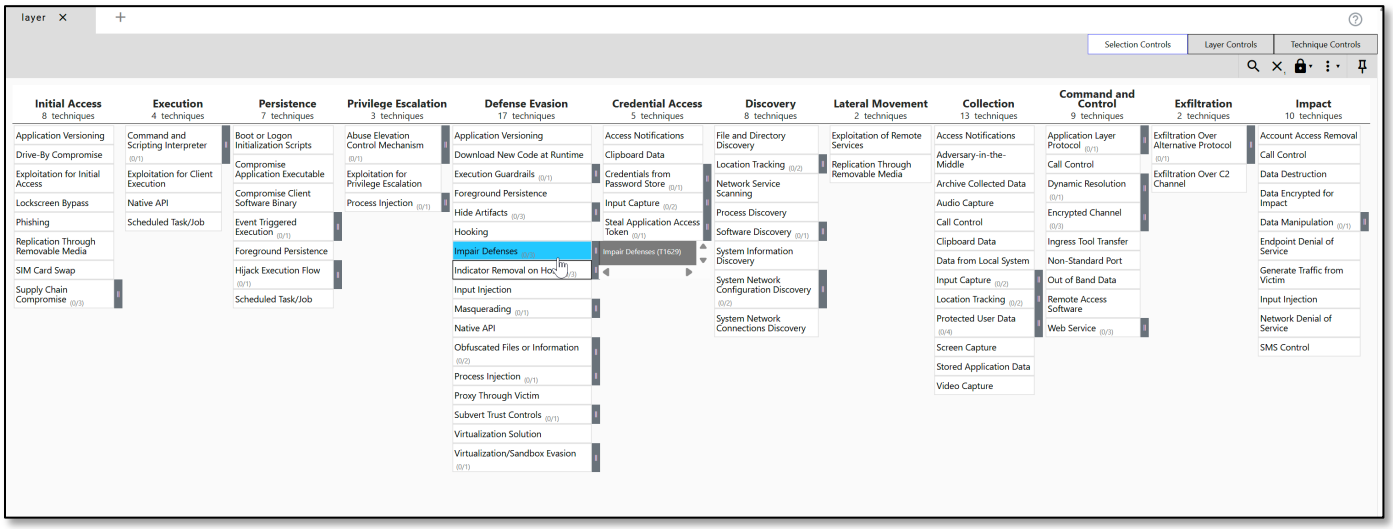


Figure 21: MITRE ATT&CK Navigator WebUI

Portainer (containerized applications)

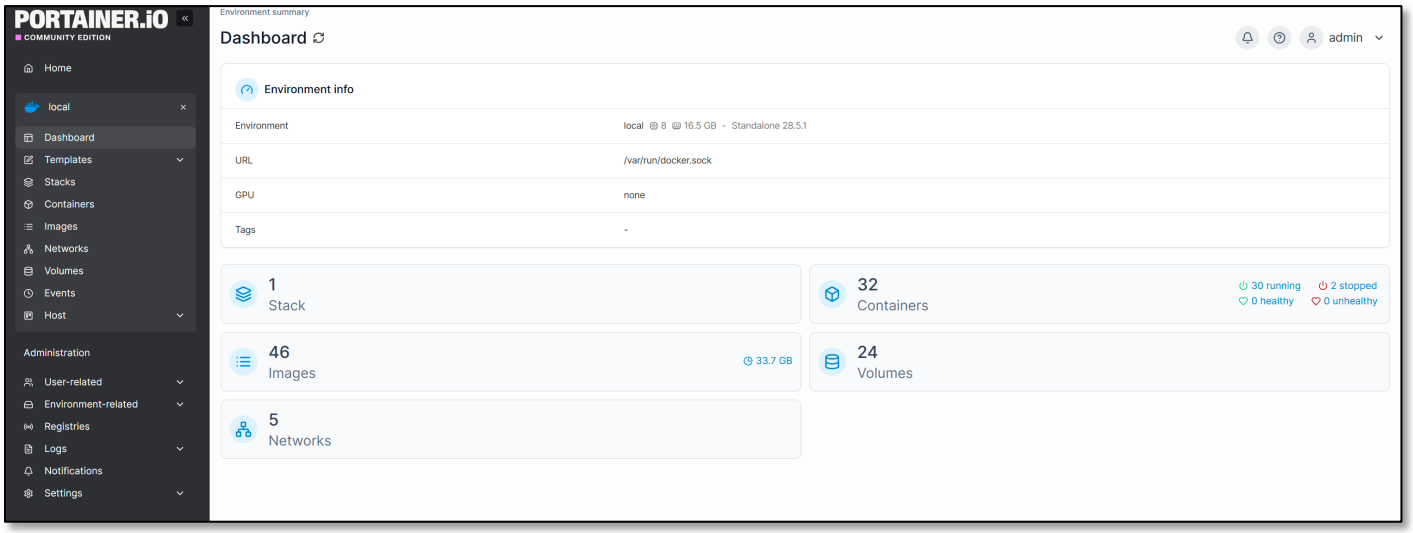


Figure 22: Portainer WebUI

Deploying Agents

Agent Deployment Center

See the following Screenshot for Agents tab showing all deployment options

The Agents tab provides one-click deployment packages for:

Velociraptor (DFIR Agent)

1. Download pre-configured packages for:
   - Windows (velociraptor-windows.exe)
   - Linux (velociraptor-linux)
   - macOS Intel (velociraptor-macos-intel)
   - macOS ARM (velociraptor-macos-arm)
2. Install on target endpoint using the installation guide in the package.
3. Agent auto-connects to your server!

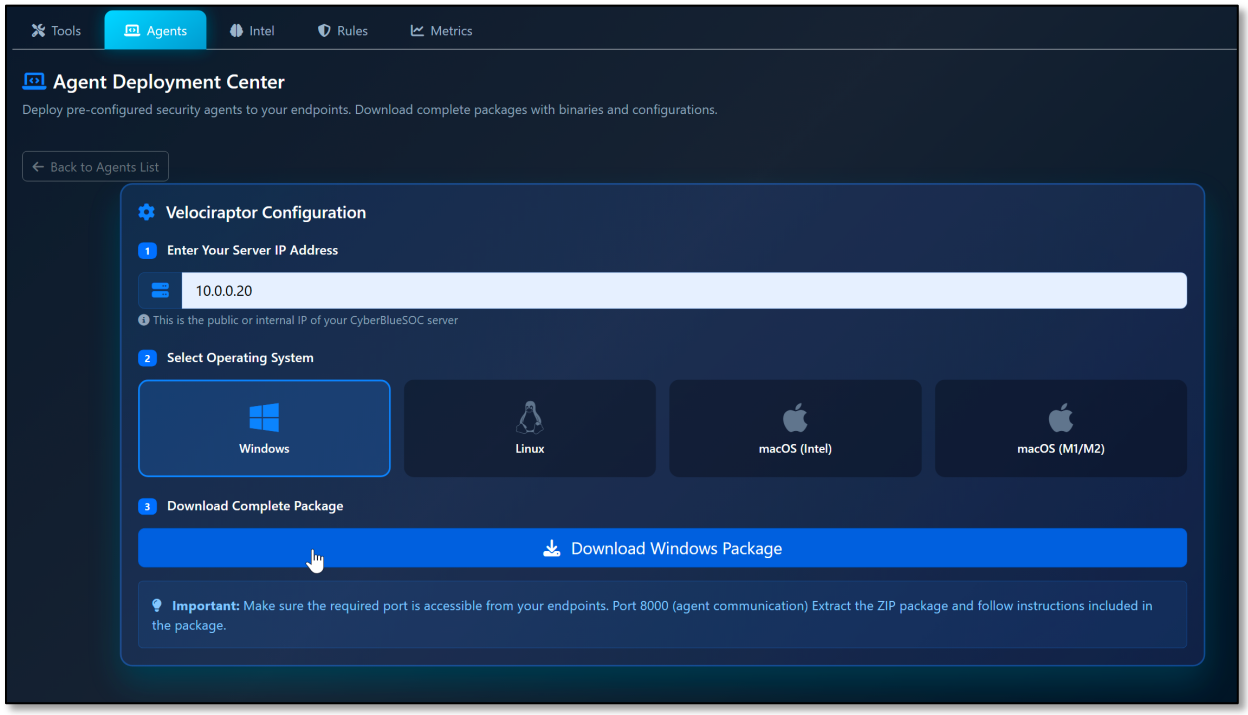


Figure 23: Velociraptor Agent Deployment

Wazuh (SIEM Agent)

The following screenshot shows the configuration wizard Steps:

1. Enter your server IP (e.g., 10.0.0.20)
2. Select OS: Windows / Ubuntu-Debian / RHEL-CentOS
3. Click "Download Windows Package" (or Linux/macOS)
4. Install on target endpoint using the installation guide in the package.
5. Agent auto-connects to your server!

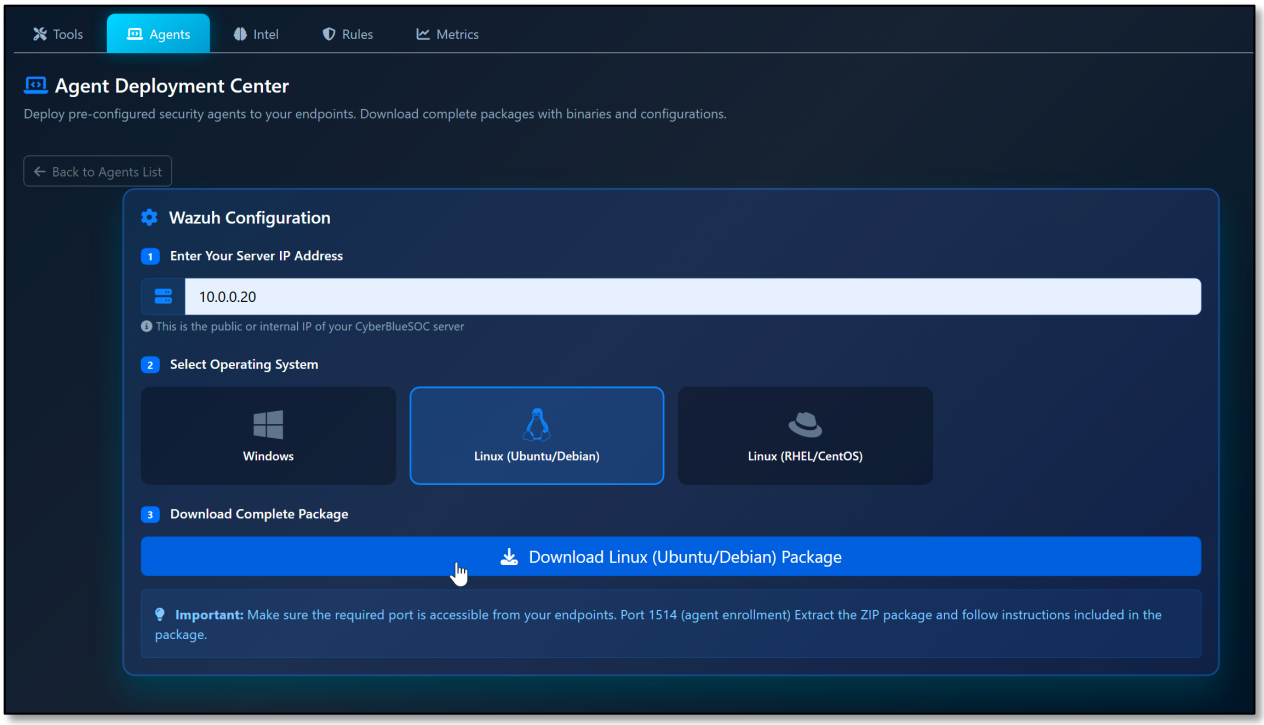


Figure 24: Wazuh Agent Deployment

Arkime Network Capture (PCAP)

1. Select Arkime PCAP from the Agents tab
2. Select the Capture duration and start capturing traffic
3. Open in Arkime to see the captured packets

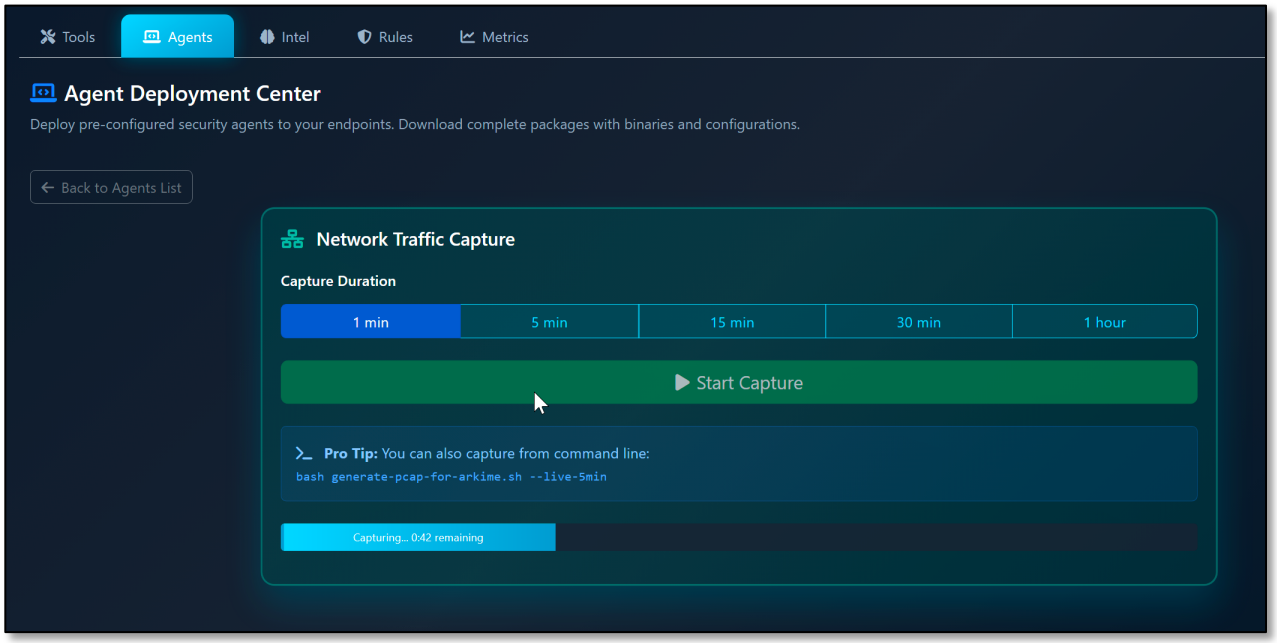


Figure 25: Arkime PCAP Generator

Threat Intelligence

IOC Search Interface

See the following creenshot Intel tab with search and results

Search 250,000+ threat indicators instantly:

Search for:

a. IP addresses

b. Domain names

c. File hashes (MD5, SHA1, SHA256)

d. URLs

Test buttons included:

e. Test: IP (pre-loaded malicious IP)

f. Test: Domain (example domain)

g. Test: Hash (malware hash)

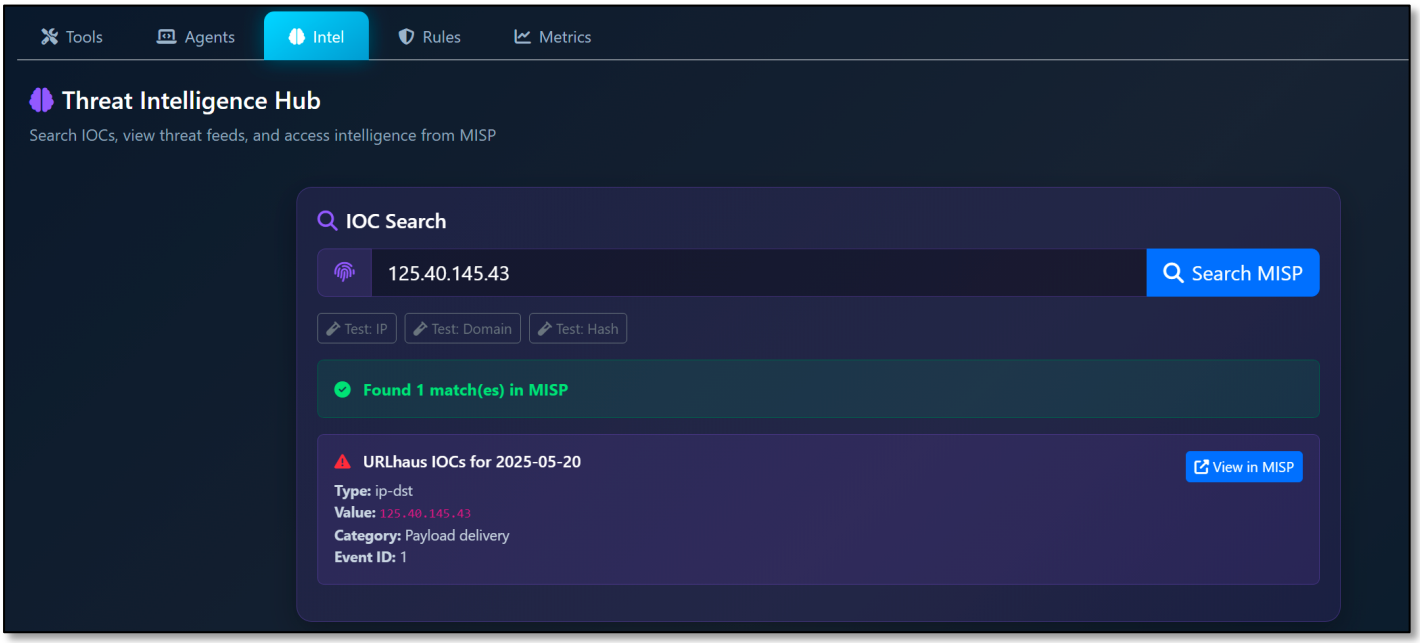


Figure 26: MISP IOC Search

MISP Statistics Dashboard

Visible in the following screenshot

Live metrics:

h. **20 Events** - Threat Event groups/campaigns

i. **250k+ Attributes** - Individual IOCs

j. **4 Active Feeds** - Auto-updating sources

Click "Open MISP Dashboard" for full threat intelligence interface.

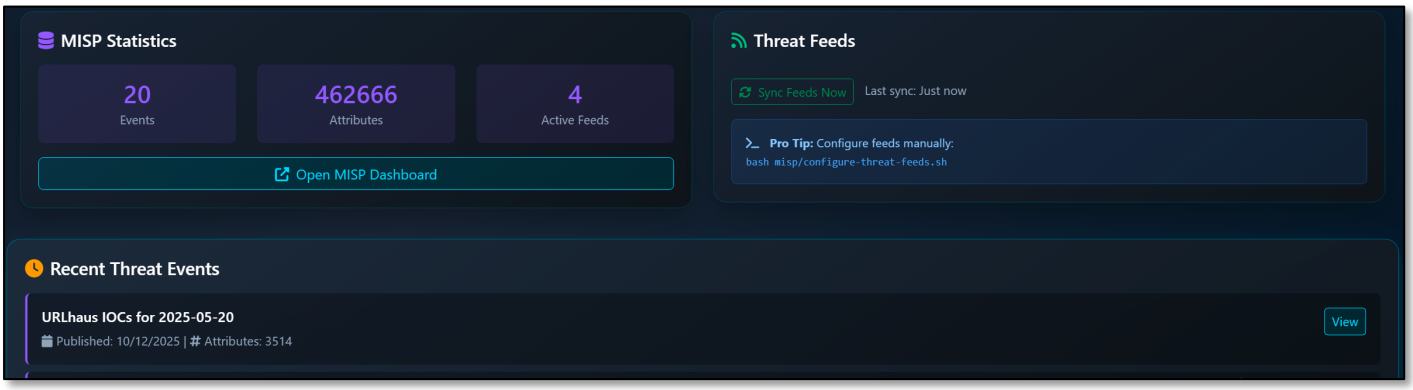


Figure 27: MISP statistics

Detection Rules

YARA Malware Detection

See the following Screenshots, Complete rules browser interface

523 rules across categories:

Category	Rules
malware	363
deprecated	66
maldocs	20
exploit_kits	11
packers	6
webshells	9
cve_rules	14
crypto	1

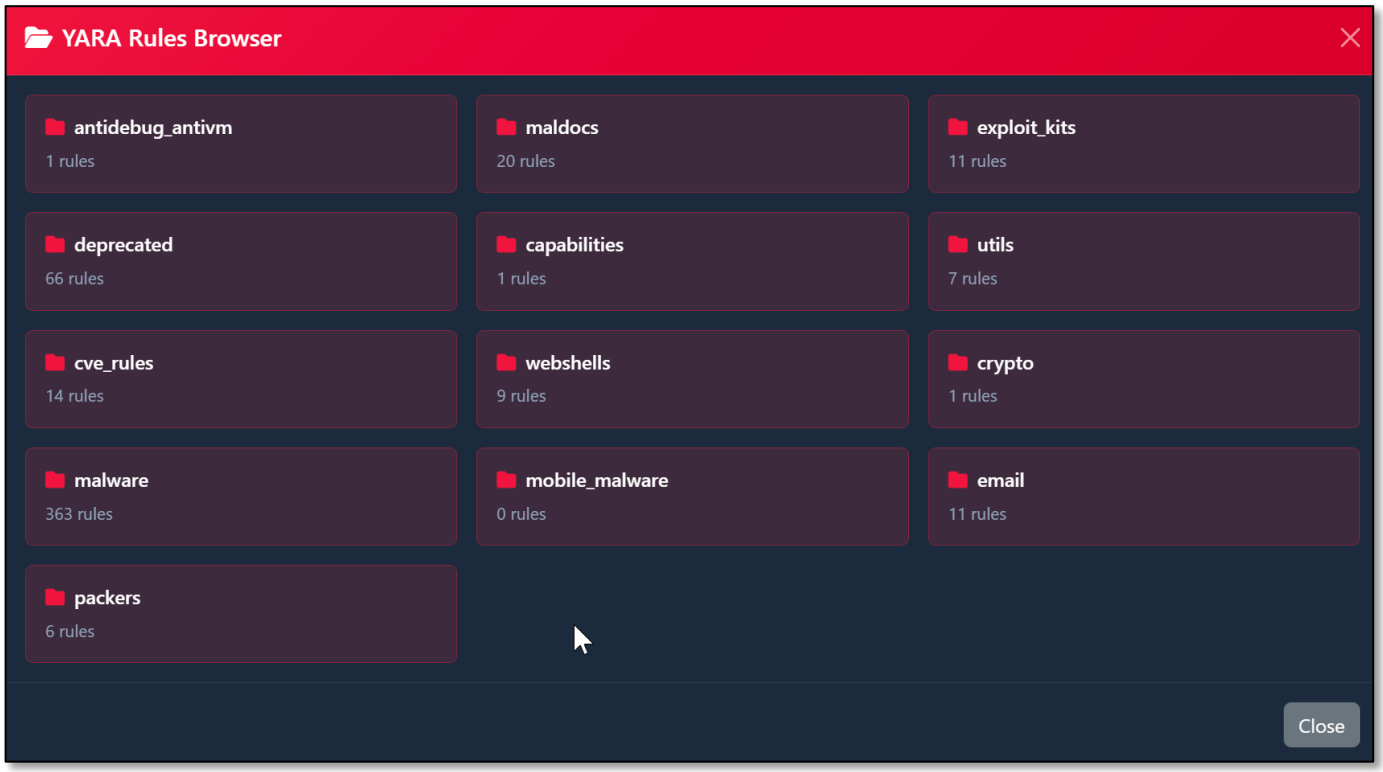


Figure 28: YARA Rules Categories browser

The following screenshot shows the YARA browser with a red-themed interface displaying all categories as clickable tiles.

Browsing rules:

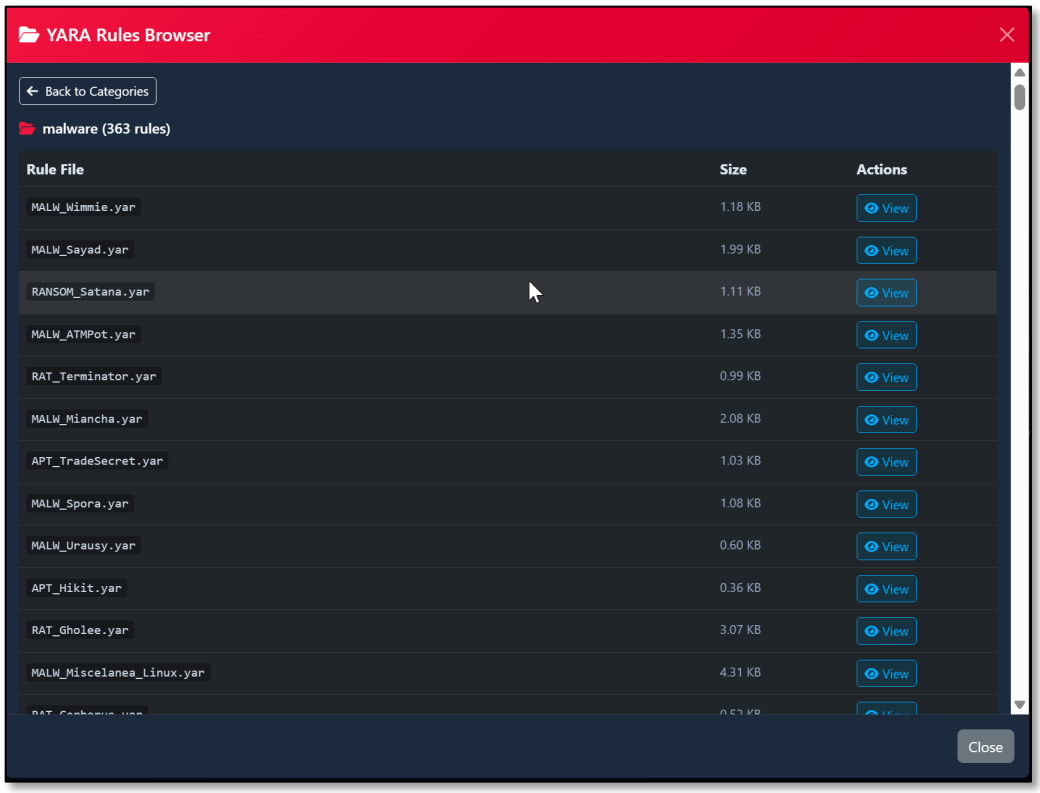


Figure 29: YARA Rules Browser

Viewing rule content:

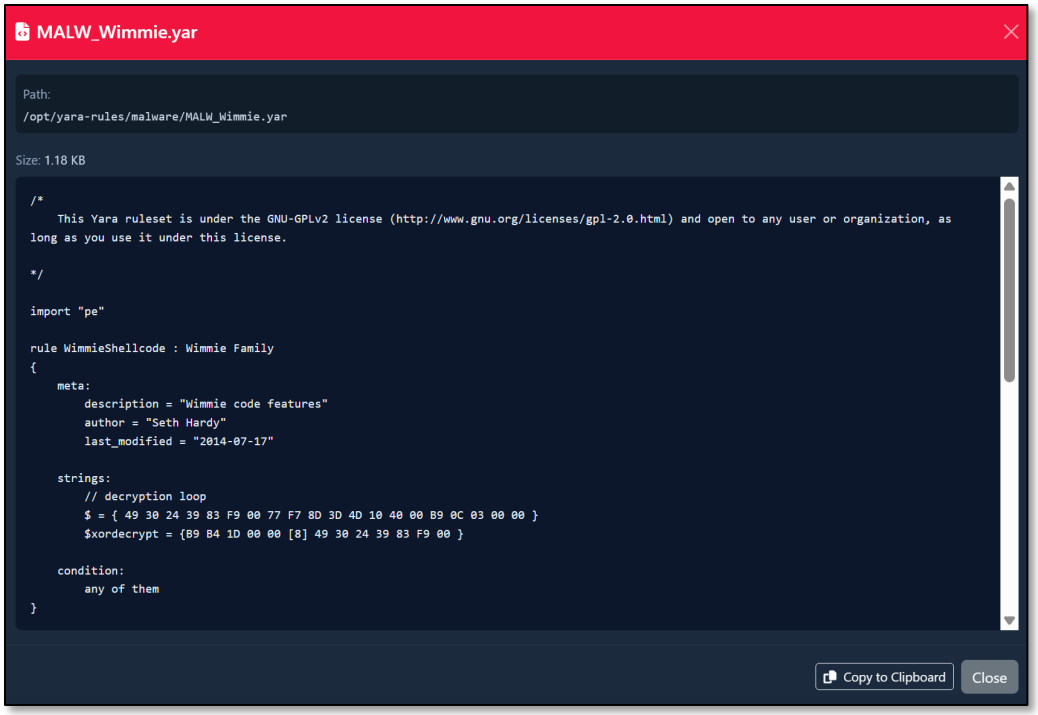


Figure 30: YARA Rule Content

Sigma Detection Rules

3,047 rules for multiple platforms:

Platform	Rules
windows	2,338
cloud	269
linux	206
macos	89
application	63
network	47
web	45

The following screenshots shows the Sigma browser with a blue-themed interface. The next Screenshot displays cloud- specific rules like aws_enum_buckets.yml for detecting bucket enumeration attacks on AWS CloudTrail.

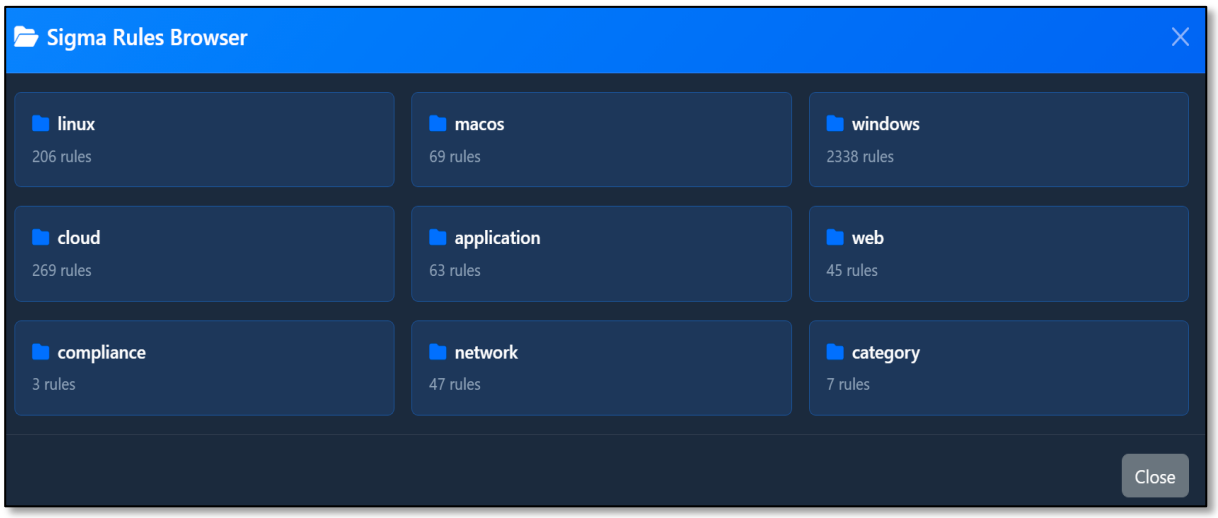


Figure 31: Sigma Rules Categories

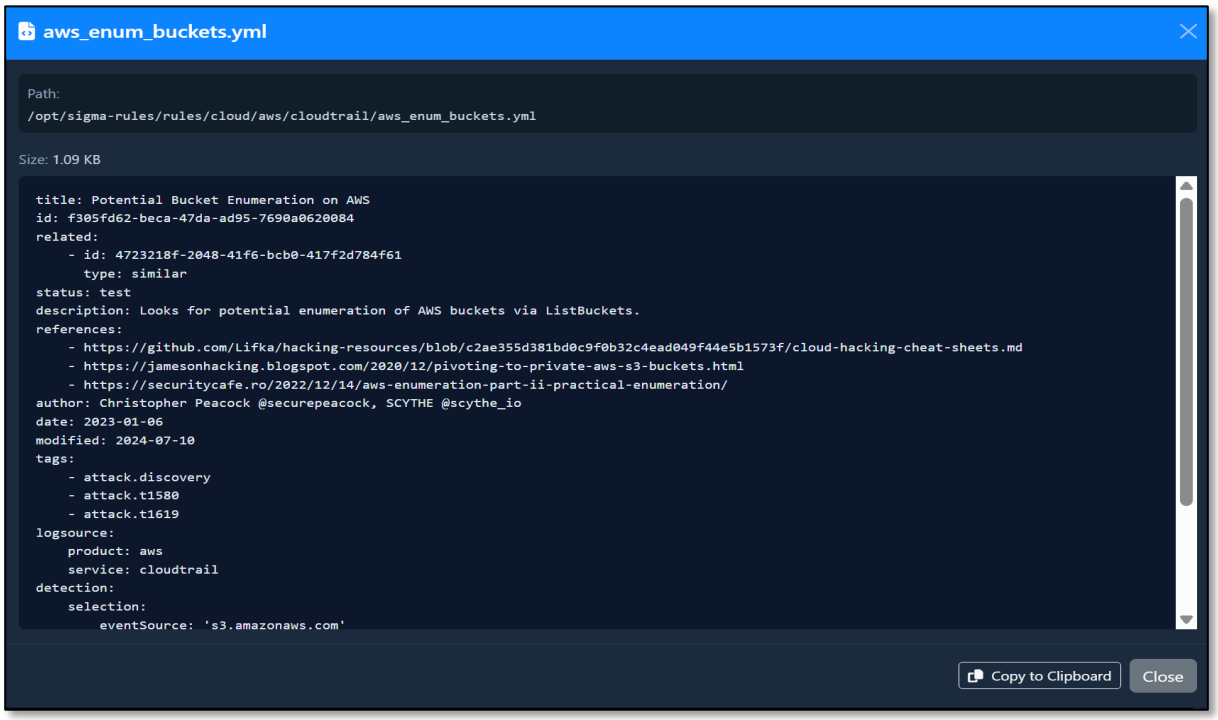


Figure 32: Sigma Rule Content

System Monitoring

Metrics Dashboard

See the following Screenshot: Complete system metrics interface

Four key performance gauges:

- **CPU Usage:** Real-time processor utilization
- **Memory Usage:** RAM consumption monitoring
- **Disk Usage:** Storage space tracking
- **Network I/O:** Total data transfer

Container Status Grid:

Visual overview of all 30+ containers:

- Green = Running healthy
- Red = Stopped
- Each container shows name and uptime

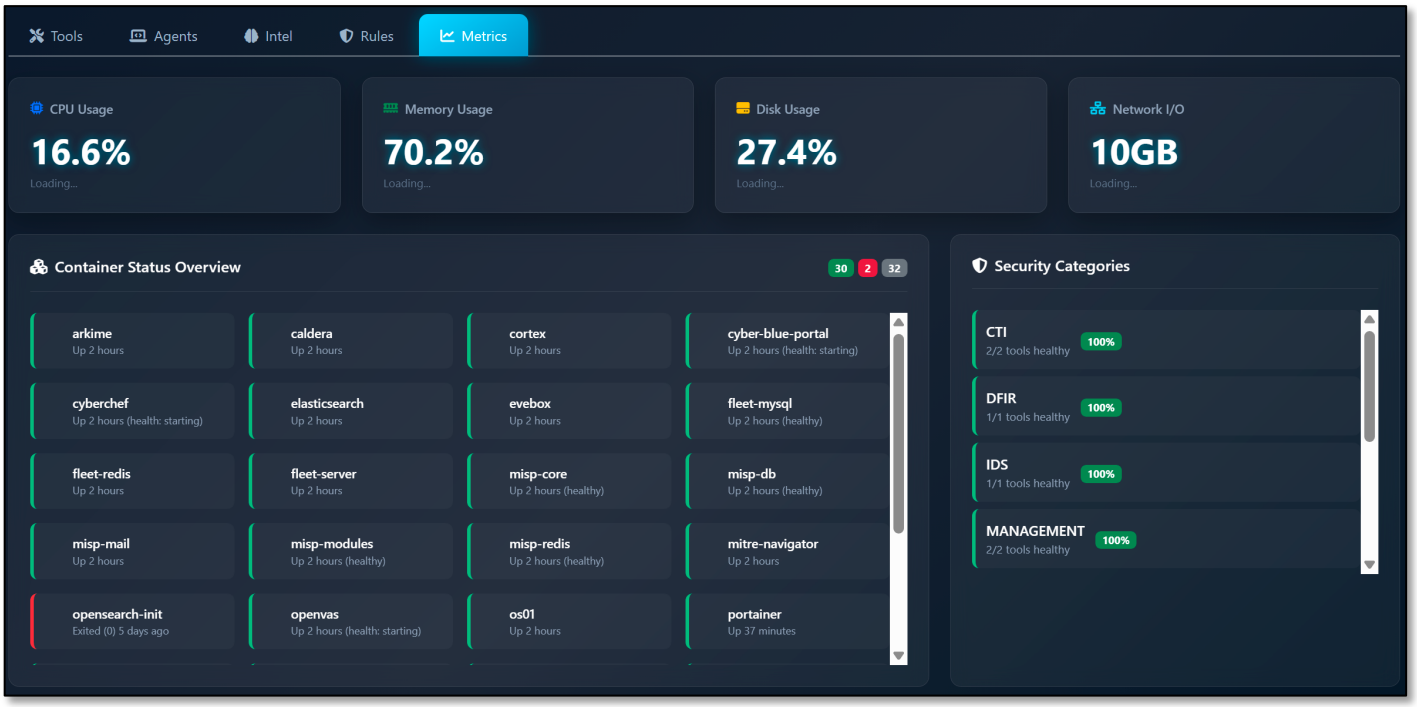


Figure 33: CyberBlueSOC Metrics Dashboard

Troubleshooting

All tools stopped?

```
./force-start.sh
```

Check logs:

```
sudo docker logs [container-name]
```

Restart specific tool:

```
sudo docker-compose restart [service-name]
```

Get back to the following full troubleshooting guide:
https://github.com/cyberblu3s/CyberBlue/blob/main/docs/TROUBLESHOOTING.md

Quick Reference

Essential Commands

```
# Check all containers
sudo docker ps

# Restart all services
sudo docker-compose restart

# Emergency restart
./force-start.sh

# Update threat feeds
bash misp/configure-threat-feeds.sh
```

System Locations

YARA Rules: /opt/yara-rules/
Sigma Rules: /opt/sigma-rules/
Project: ~/CyberBlue/

Common Issues & Solutions

Reference: Get back to the following full troubleshooting guide:
https://github.com/cyberblu3s/CyberBlue/blob/main/docs/TROUBLESHOOTING.md

Installation Problems

Port Already in Use

Problem: Error message: "bind: address already in use"

Solution:

```
# Find what's using the port
sudo lsof -i :7001

# Kill the process
sudo kill -9 [PID]

# OR change port in docker-compose.yml
```

Out of Disk Space

Problem: "no space left on device"

Solution:

```
# Check space
df -h

# Clean Docker
sudo docker system prune -a -f

# Remove old images
sudo docker image prune -a -f
```

Docker Permission Denied

Problem: "permission denied while connecting to Docker daemon"

Solution:

```
# Add user to docker group
sudo usermod -aG docker $USER

# Re-login or run:
newgrp docker

# Verify
docker ps
```

Runtime Issues

Container Keeps Restarting

Problem: Container shows "Restarting" status

Solution:

```
# Check logs
sudo docker logs [container-name]

# Common fixes:
# 1. Memory issue - check swap
free -h swapon
--show

# 2. Config error - restart container
sudo docker-compose restart [container-name]

# 3. Dependency issue - restart all
./force-start.sh
```

Portal Not Loading

Problem: Can't access https://IP:5443

Solution:

```
# Check portal container
sudo docker ps | grep portal

# Restart portal
sudo docker-compose restart portal

# Check logs
sudo docker logs cyber-blue-portal

# Verify port not blocked
sudo ss -tulpn | grep 5443
```

Tool Shows "Stopped"

Problem: Tool card shows red "Stopped" status

Quick Fix: - Click green "Start" button on tool card - Wait 30 seconds - Refresh page

If that doesn't work:

```
sudo docker-compose restart [service-name]
```

Performance Issues

High Memory Usage

Problem: System using >90% memory

Solutions:

```
# Check memory
free -h

# Restart memory-heavy services
sudo docker-compose restart wazuh-indexer
sudo docker-compose restart shuffle-opensearch

# Add more swap if needed
sudo fallocate -l 16G /swapfile2
sudo chmod 600 /swapfile2
sudo mkswap /swapfile2
sudo swapon /swapfile2
```

Slow Portal Response

Problem: Portal feels sluggish

Solutions: 1. **Check container count:**

```
sudo docker ps | wc -l        # Should be 30+
```

2. **Restart Docker:**

```
./force-start.sh
```

3. **Check system resources in Metrics tab**

MISP Issues

No Threat Indicators Problem: MISP shows 0 attributes

Solution:

```
# Manual feed sync
cd ~/CyberBlue
bash misp/configure-threat-feeds.sh

# Check logs
tail -f /var/log/misp-feed-sync.log

# Wait 10-15 minutes for download
```

Can't Login to MISP

Problem: MISP requires password change

Solution:

```
# Already configured - use: # admin@admin.test / admin
# If still issues, reset:
cd ~/CyberBlue
bash force-create-misp-admin.sh
```

Network Issues

Suricata Not Capturing Problem: EveBox shows no events

Solution:

```
# Update network interface
cd ~/CyberBlue
./update-network-interface.sh --restart-suricata
# Verify interface
ip route | grep default
# Check Suricata logs
sudo docker logs suricata
```

Can't Access Tools from Remote

Problem: Tools work on localhost but not from other computers

Solution:

```
# Check firewall (for cloud deployments) # AWS: Update Security Group
# Azure: Update Network Security Group # GCP: Update Firewall Rules
# For Ubuntu UFW:
sudo ufw allow 5443/tcp
sudo ufw allow 7000:7099/tcp
sudo ufw allow 9443/tcp
sudo ufw enable
```

CyberBlueSOC!

Your SOC & Blue team journey can starts now!
Happy hunting!